APPARATUS FOR SELECTING AND DISPLAYING A FILE ASSOCIATED WITH A CURRENT GEOGRAPHIC LOCATION

CROSS REFERENCE TO RELATED APPLICATIONS

This application is a divisional of U.S. patent application Ser. No. 12/868,722 filed on Aug. 26, 2010, which is a continuation-in-part of U.S. patent application Ser. No. 12/546,881 filed on Aug. 25, 2009. The entire contents of both of these applications are incorporated herein by reference.

BACKGROUND

1. Field of the Invention

The field of the invention relates to portable electronic devices and more particularly to the security of information kept within portable devices.

2. Background of the Invention

Fraud prevention methods are well known. In the past, methods of fraud prevention were based upon a personal relationship among transaction partners. Merchants knew their customers and would not be fooled by someone else asking for access to customer accounts.

In today's environment, merchants and account managers do not personally know their customers. As such, access to accounts is typically based upon at least two levels of security. On the first level, a user is required to have some form of identification (e.g., a credit or debit card, an account number, etc.). The second level of security is usually a password.

The first level of security is often manifested in a hard-coded format (e.g., a plastic card) that could be lost or stolen. On the other hand, the second level of security (i.e., passwords) are often committed to memory. As long as a person's password is committed to memory, a lost or stolen credit card is useless.

However, many people often forget their passwords. As a consequence, some people will write their passwords down and carry the passwords with them in their purse or wallet. In this case, if the user loses their purse or wallet, then a thief may still be able to access the accounts of the account holder.

In order to counteract the problem of compromised passwords, many organizations will often request personal information from users (e.g., mother's maiden name, high school mascot, name of first employer, etc.). In addition, to requiring an account number and passwords, many organizations often request an item of personal information on a random basis.

While adding another level of security further increases security, the additional level further increases the difficulty in providing the information of the various levels of security, especially where the memory of a user is impaired. This problem is made worse when a user has accounts with many different organizations. Accordingly, a need exists for better methods of providing the information required for the various levels of security.

SUMMARY OF THE INVENTION

According to one aspect of the present invention, an apparatus includes at least one storage device that stores a plurality of files wherein each file contains at least one item of confidential information and wherein a geographic location of use is associated with the file; a position comparison processor coupled to the at least one storage device that compares a current geographic location with each of the geographic locations of use associated with the plurality of files; and a display coupled to the position comparison processor that displays contents of a selected file, wherein the geographic location of use associated with the selected file matches the current geographic location.

Other aspects of the inventions will be apparent upon review of the disclosure contained herein.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. **1** is a block diagram of a password protection system **10** shown in a context of use generally in accordance with an illustrated embodiment of the invention;

FIG. **2** is a master password entry screen that may be used by the system of FIG. **1**;

FIG. **3** is a title selection list screen of confidential information that may be displayed by the system of FIG. **1**;

FIG. **4** is confidential information for a title selected by a user from the screen of FIG. **3**;

FIG. **5** is a settings screen that may be selected by a user through the screens of FIG. **3** or **4**;

FIG. **6** is a synchronization screen that may be selected by a user through the screens of FIGS. **3-5**;

FIG. **7** is an Import/Export screen that may be selected by a user through the screens of FIGS. **3-6**;

FIG. **8** is a master password entry screen of a portable device that may be used by the system of FIG. **1**;

FIG. **9** is an introductory title list screen of a portable device that may be used with the system of FIG. **1**;

FIG. **10** is a selection list screen of confidential information of a portable device that may be displayed by the system of FIG. **1**;

FIG. **11** is an information screen of a portable device that may be selected through the screen of FIG. **10**;

FIG. **12** is an edit screen that may be selected through the screen of FIG. **11**; and

FIG. **13** is a synchronization screen that may be selected through the screens of FIGS. **9-12**.

FIG. **14** is a flowchart illustrating optional programming executed by the password protection system **10** according to a further embodiment of the present invention;

FIGS. **14A-14C** are screenshots of screens presented to a user associated with the programming of FIG. **14**;

FIG. **15** is an alternative settings screen similar to FIG. **5** that permits selection of settings, including an asynchronous auto-sync function, for the system of FIG. **1**;

FIGS. **15A-15H** are screen shots of alternative screens presented to user for an alternative method of implementing synchronization and database backup routines;

FIG. **16** is a flowchart of programming executed by the system of FIG. **1** to implement the asynchronous auto-sync operation;

FIG. **17** is a synchronization screen similar to FIG. **13** that permits a user to request deletion of records on a lost or stolen device;

FIG. **18** is a flowchart of programming responsive to actuation of a softkey of FIG. **17** to delete selected records on a lost or stolen device;

FIG. **19** is an Import/Export screen similar to FIG. **7** that permits a user to request transmission of selected records to another user;

FIG. **20** is a flowchart of programming executed by the system of FIG. **1** in response to actuation of a softkey of FIG. **19** that transmits records to a second user; and

FIG. **21** is a flowchart of programming that may be executed by the system of FIG. **1** operating on a second user's device that permits the second user to receive records from the first user.